INTEROPERABILITY

ASSESSMENT

Presented to the:

66th MORS Symposium
Naval Post Graduate School
Monterey, California
23-25 June 1998

19980805 141

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

Litton
PRC

Michael J. Leite, PE
PRC, Inc.
2361 Jefferson Davis Highway
Arlington, Virginia 22202-3876

DTIC QUALITY INSPECTED 1

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA, 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188, Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
8 June 1998

3. REPORT TYPE AND DATES COVERED
Technical Report, May--June, 1998

4. TITLE AND SUBTITLE
Interoperability Assessment

5. FUNDING NUMBERS

6. AUTHOR(S)
Michael J. Leite

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
PRC, Inc.
2361 Jefferson Davis Highway (Suite UL330)
Arlington, VA 22202-3876

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joint Theater Air and Missile Defense Organization (JTAMDO)
Department of Defense
Washington, DC 20301

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This paper describes a methodology that resolves system interoperability deficiencies through the measurement and quantification of a set of interoperability system components. The objective assessment of interoperability thus becomes the sum of the assessments for the individual characteristics.

14. SUBJECT TERMS
Interoperability, Assessment, Performance Measurement

15. NUMBER OF PAGES
14

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	19. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	NONE

NSN 7450-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Sta. 239-18
298-102

DTIC QUALITY INSPECTED 1

INTEROPERABILITY

ASSESSMENT

Presented to the:

66th MORS Symposium
Naval Post Graduate School
Monterey, California
23-25 June 1998

Litton

PRC

Michael J. Leite, PE
PRC, Inc.
2361 Jefferson Davis Highway
Arlington, Virginia 22202-3876

INTEROPERABILITY ASSESSMENT

I BACKGROUND

In February 1998 CINCLANTFLT stated "It appears from the fleet that, for combat systems, there is no focus on battle group and Joint interoperability..." and "...they have failed to deliver integrated warfighting capability to our battle groups."[(1)] This indicates that there has been little change since the VCNO stated in 1985 that "... the Navy has a fragmented approach to the implementation of Battle Force Command and Control systems from a lack of understanding of system interoperability issues and programmatic actions being taken without full understanding of the impact on interrelated programs..."[(2)]

Serious interoperability deficiencies exist today. They have been perpetuated across all the services and have been identified in all recent, allied, joint and combined operations and exercises. Interoperability is often considered to be a desired, but unattainable, goal rather than a condition which can be quantified.

This paper describes a methodology that resolves system interoperability deficiencies through the measurement and quantification of a set of interoperability system components. The objective assessment of interoperability thus becomes the sum of the assessments for the individual characteristics.

II INTEROPERABILITY DEFINED

The *Department of Defense Dictionary of Military and Associated Terms*[(3)], Joint Pub 1-02, defines interoperability as:

> "1. The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together." and
>
> "2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to separate areas."

Using the foregoing, a set of interoperability components can be identified which will provide a measure of system interoperability. They are the following:

Requirements	Information Flow
Standards	Latency
Data Elements	Interpretation
Node Connectivity	Information Utilization
Protocols	

III Degree of Interconnection

1. Interoperability does not just happen. It is achieved in several well defined steps like the rungs on a ladder. Interoperability is described by several degrees of interconnection, each of which has a unique set of characteristics. The degrees are discussed individually in the following:

a. Connectivity--*There is a medium which connects us.* At this degree we can only sense the presence of the other node. The key elements are:

(1) Common medium

(2) Transmitter

(3) Receiver

(4) Interface Description

An example of simple connectivity is the test patten generated by a television station or a continuous tone generated by a radio station. Only the operability of the medium is conveyed.

b. Availability--*The medium is available whenever we wish to communicate.* This adds the element of control to the medium in that the link may be operated at the discretion of the nodes. The added elements are:

(1) Transmission protocols

(2) Schedule

(3) Common cryptographic key

The availability of a medium is determined by the presence of a transmitter and receiver who are simultaneously ready to exchange data. For broadcast media, this is established through the use of published schedules. With tactical data links, availability may be governed by a polling sequence, the assignment of fixed time slots or a permission/interrogation scheme.

c. Interpretation--*When you tell me something, I can correctly interpret the data elements.* At this degree, information is passed between the nodes. Common data bases can be maintained and common track files and displays are possible. Four elements are added at this point:

(1) Common data elements

(2) Common message formats

(3) Reporting responsibility (R^2) rules

(4) Message Standards

To be useful, data must be understood. To accomplish this, the structure of the transmitted data must be rigidly structured with both transmitter and receiver making a common interpretation of the structure. For voice transmission examples are amplitude modulation, frequency modulation and single-sideband. For data transmissions we are concerned with pulse width and amplitude, the number of pulses per element of data and the structure of data elements into messages. Data must be unambiguous and provide sufficient redundancy as to permit error identification and correction.

d. Understanding--*When you tell me what you are doing, I can understand your actions*. "Interpretation" above added "nouns and adjectives" to the system; they permit the description of "things." The "understanding" degree adds "verbs and adverbs;" they allow the description of "actions" such as maneuvering and engaging the enemy. The nodes know what the others see and what they are doing. Elements attributable to this degree are:

(1) Data rates

(2) Timeliness or data latency

The transition from the simple exchange of data to the communication of actions implies an element of timeliness to the data transmission. At some point the communication will become stale and lose its utility. The acceptable latency for a data stream is determined by the action which must be initiated by the recipient upon its arrival.

e. Execution--*You can cause me to take action.* At this degree one system takes control of all or part of a remote system and executes functions of that system. The element added at this degree is:

(1) Command (executable instructions)

The concept of execution implies the transmission of a command or "executable instruction" to the recipient. A simple example is the operation of the remote control for a television; another is the use of powerline carriers to turn lights and appliances on and off. At its most complex implementation, one combat system is directing a remote sensor to search for a target or commanding a weapon system to engage a target. Positive control is a key concern with respect to execution; errors can cause fratricide or self-inflicted damage to the remote unit.

f. Feedback--*I can report what has been done.* As opposed to the data exchange discussed previously, feedback reports the response to commands or system actions. It is not simply a routine data exchange. Element of feedback are:

(1) Confirmation (receipt and execution)

(2) Consequences (results)

Whenever actions are initiated, feedback is required to ensure that the correct action was initiated and that it had the desired effect. In the case of the remote controls, the results were observed directly. In the case of the tactical engagement, the report must be received via a tactical data link. An important consideration is that the command and the feedback DO NOT have to utilize the same medium. In the commercial world, in which remote users utilize low bandwidth media (telephone) for outgoing data and high bandwidth media (satellite) for reception.

IV INTEROPERABILITY COMPONENTS

1. Requirements. All systems or components, for which interoperability is desired, must have common operational requirements. Without such requirements, system developers and acquisition managers have no obligation to deliver interoperable systems. Three levels of interoperability which can be specified are:

a. Data. Data elements are exchanged between systems which implement and maintain common, distributed data bases.

b. Command and Control. Command and Control (C^2) information is exchanged between systems; requests are received and processed. Action is initiated locally and reported globally over integrated communications broadcasts and networks.

c. Execution. One system takes control of all or part of a remote system and executes functions (detect, control, engage) of that system.

A review of a system's Operational Requirements Document will determine the existence of system interoperability requirements. To ensure the implementation of the requirements, they must be traced to the lowest specification level; this may be accomplished manually or through the use of automated tools like *SpecWriter*™[4] and DOORS™[4]. For all requirements criteria must be developed to demonstrate conformance with the operational requirements.

The first step in measuring compliance with the requirements is to trace the requirements through the system functions. This may be accomplished by the development of "operational threads" (system node connectivity or link/node diagrams) or paths between the systems. The threads are identified, traced, and developed in order to measure and quantify system interoperability. Consequently, interoperability deficiencies can be determined before the system is fielded.

2. Standards. Interoperability standards define the transmit node, receive node, the specific message content, and the media that carries the data (data link) between the nodes. To be interoperable, the systems must have a common implementation of the standards. This requires that the same editions of the standards be installed in all the system nodes. Since all node functionalities are not common to all interoperable systems, implementation of the standards may be partial; however, for those functionalities which are common, the implementation must be identical. Interoperability also requires that nodes, which partially implement the standards, be capable of accepting and passing all message content covered by the standards if they are required to relay to other systems.

A transparent "Plug and Play" capability, as is proposed for Athena, Common Host Software and JAVA Technology, is required for full system interoperability implementation. For those systems where common codes and algorithms have not been implemented, their interoperability may be established through the application of Distributed Interactive Simulations (DIS) including hardware-in-the-loop and human-in-the-loop testing. In this way the systems may be connected in a simulated environment and their interoperability tested against "standard" scenarios.

3. Data Elements. Thus far we have examined the requirements and standards. If the assessments in those areas are positive, we can assert that information flows between nodes in a common format at adequate data rates. Interoperability, however, is not yet assured. The next step is to assess the content of the data stream.

Evaluating the data stream is a verification and validation (V&V) process. Several procedures exist for the conduct of verification and validation; perhaps the most rigorous is the Fourteen Step Process developed by PRC, Inc.[5] The key objectives of the process are the following:

a. Common definitions are used for each data element. This includes a common reference for reporting observations--time, coordinate system, units.

b. Common, or published, measurement accuracy and reporting precision for data elements.

c. Known or transmitted covariances for reported data.

d. Common correlation/association conventions for track designations.

The analysis begins with each message set and examines the individual data elements. Usong the Fourteen Step Process, the logic is traced from the generation of the data to the receipt and input of the data into each of the receiving nodes. And, the application of each data element by the receiving nodes is traced. The process establishes that all nodes have a common understanding of the data content.

4. Node Connectivity. Because node connectivity is a function of time, both continuous and discrete time intervals, it is often one of the most difficult elements of interoperability to

measure. In simple terms, connectivity is the ability to send and receive data at any time. This implies that the transmitter and receiver are both up and that the link is available. For any interoperable system the operator has control of the medium and equipment; the environment represents those items which are outside the operator's direct control.

The medium includes the transmission path (copper wire, coaxial cable, fiber optics, the atmosphere or water), the frequency spectrum (direct current to light) and the wave form (AM, FM, etc.). Each medium has its strengths and weaknesses. As the wavelength decreases, the data rate increases; however, at the same time, the propagation approaches line of sight and attenuation increases. Environmental effects also vary as a function of wavelength.

The environment includes atmospherics, noise, obstructions, interference/jamming. Models exist for the calculation of propagation and losses through the atmosphere as a function of the atmosphere, weather, land masses and sunspots. Similarly models exist for the prediction of propagation losses through conductors, wave guides and fibers as well as for acoustic propagation.

Equipment is a key variable in the estimation of interoperability. First, because units come from multiple services and countries there is only limited commonality. Second, even with units from the same service, equipment suites are often comprised of different models with varying capabilities. Particularly with late model equipment, it is the software loads which are different. The criterion for interoperability is compatibility; specifically, the equipment must utilize a common waveform and cryptographic load and be able to generate a common input or output in a format which the users can accept and utilize.

Connectivity varies continually during an operation or exercise. In post event analysis or reconstruction it is possible to quantify the connectivity throughout the event. It is possible to estimate connectivity on a real time basis. Prior to an event an estimate can be made with respect to connectivity based upon the environmental conditions. For any communications structure, a connectivity index can be defined.[6] It is a relationship between the number of system nodes and the available paths. The Connectivity Index is defined by the equation:

$$C_I=\frac{k}{n\times(n-1)} \tag{1}$$

Where:

C_I = Connectivity index
k = Number of connections (paths) between nodes
n = Number of nodes (participating units)

A connectivity index can be calculated for any communications system; however, the values calculated for one type of system (Link-11) are not indicative of performance on another system (e.g.: Link-16) for which the same value of "C" is calculated.

Connectivity can be measured directly by counting the number of messages initiated by all participating units and the number of messages received for the network or data link. To the extent that the Link is in continuous operation, the connectivity sampled in this manner is representative of network connectivity. If the network is operated intermittently, then the sample must be carefully selected and tested to ensure that the required confidence level is attained. The general relationship for measuring the connectivity is the following:

$$C = (1/n_r) \times \frac{\sum_{y=1}^{n_r} (M_r)_y}{\sum_{x=1}^{n_t} (M_t)_x} \qquad (2)$$

Where:

C = Node Connectivity (during measurement period)
n_r = Number of receiving nodes
n_t = Number of transmitting nodes
M_t = Messages transmitted by a node
M_r = Messages received by a node

5. Protocols. Protocols determine access to a data stream. On the transmit side, the protocol establishes polling sequences, transmit time allocations and the data which may be transmitted. On the receiving side the protocols determine the data which is filtered out or passed to the user. The protocols are based on the information exchange requirements, the volume of data to be passed and the available datalink/processor capacity.

Information exchange requirements define the data to be passed, the sources/destinations of the data, its uses and the acceptable latency for the data (based on user requirements).

The adequacy of protocols is typically established by tracing the logic in the algorithms using the information exchange requirements; then the package is tested using simulations for individual nodes and groups of nodes.

6. Information Flow. The volume of data is typically a function of the tempo of operations and the area of interest. The area if interest (AOI) is defined by the operational commander. The tempo of operations is event-driven; however, estimates are possible based on historical and exercise results.

Capacity is a function of the available data links--flashing light, voice, radio, fiber optic. In practice multiple links or paths are available. For weapon and combat systems, there is a requirement for primary and back-up paths. In normal operation with all systems available, there is redundancy in the data which is passed. Duplicate data are filtered by either relying on the "primary" system or by filtering the data stream. For example, where Link-16 and Link-11

are both operational in a battlegroup, Link-16 is considered the primary system and Link-11 is the secondary system. In such cases there are strict protocols governing the forwarding of data from one link to another. The redundancy of data flow limits the total capacity to an amount which is less than the sum of the individual systems. This also means that degradation will be less than the fractional capacity of a system which is lost.

Several items may be measured or calculated with respect to system performance. They are capacity, system overload and data latency. The relationships for these measures are the following:

a. Capacity. The capacity of a system is the rate at which data may be passed over time. Given its operating parameters, a maximum data rate can be calculated for any system or group of systems. The maximum rate must be reduced to a effective data rate or capacity by subtracting the information overhead which must be passed to maintain the system operation. The overhead consists of synchronization messages, the jitter, synchronization, header and parity check of individual messages, and the propagation time for the messages. The overhead can account for up to half of the available capacity on a net when propagation time is included. The general relationship for system capacity is the following:

$$Q_{eff}=(Q_{\max}-Q_{oh})\times(t_f-t_p) \tag{3}$$

Where:

Q_{eff}	=	Effective System Capacity (data rate)
Q_{max}	=	Maximum Data Rate
Q_{oh}	=	System Overhead Data Rate
t_f	=	Time Slot Duration (Unit transmission)
t_p	=	Unit Propagation Time

b. System Overload. A system overload occurs when more data must be exchanged than the system is able to transmit. Typically the overload is placed in a queue and is then transmitted when capacity is available. Therefore the measure of system overload is the sum of the messages remaining in queues after their assigned transmission period for all system nodes.

$$M_{OL}=n_t\times\sum_{y=1}^{n_r}(M_q)_y \tag{4}$$

Where:

M_{OL}	=	System Message Overload
n_t	=	Number of transmitting nodes
M_q	=	Messages in Queue to be Transmitted by a node

c. Underutilization. Underutilization occurs when the system data rate/message load is less than its full capacity but messages are waiting in queues to be transmitted. This occurs when the time slot or transmission allocation to selected nodes is less than that required to clear the queue by the end of a transmission period. Similarly other nodes do not use all of their allocated time.

$$Q_{uu}=M_{OL} \tag{5}$$

For $M_{OL} \leq (Q_{eff}-Q)$

AND

$$Q_{uu}=Q_{eff}-Q \tag{6}$$

For $M_{OL} > (Q_{eff}-Q)$

Where:

Q_{uu} = System Underutilization (data rate)

Q = Measured/observed Data Rate

(Other terms as previously defined)

d. Undercapacity. Under capacity occurs when messages remain in queues and the system data rate is at the maximum.

$$Q_{uc}=(Q+M_{OL})-Q_{eff} \tag{7}$$

Must be > 0

Where:

Q_{uc} = System Undercapacity (data rate)

(Terms as previously defined)

7. **Data Latency.** In strict terms, the data latency is the elapsed time from the time of the event to the time of receipt by the user (tactical data processor). For analytical purposes, the latency is often divided into smaller segments. Several common time periods are the following: time of event to time of observation, time of observation to completion of processing and completion of processing to time of receipt at the tactical data processor. This division is useful in situations involving a remote sensor and intermediate processing to reduce the data to a usable form (track message) prior to passing the data to the user. These relationships are expressed as follows:

$$\overline{\Delta t}=t_r-t_e \tag{8}$$

$$\overline{\Delta t_o}=t_o-t_e \tag{9}$$

$$\overline{\Delta t_m}=t_m-t_o \tag{10}$$

$$\overline{\Delta t_r}=t_r-t_m \tag{11}$$

And equation 8 may be rewritten as:

$$\overline{\Delta t}=\overline{\Delta t_o}+\overline{\Delta t_m}+\overline{\Delta t_r} \tag{12}$$

Where:

Δt	=	Time Latency
Δt_o	=	Latency of Observation
Δt_m	=	Latency of Measurement/Processing
Δt_r	=	Latency of Transmission/Receipt
t_e	=	Time of Event
t_o	=	Time of Observation
t_m	=	Time of Completion of Processing
t_r	=	Time of Receipt

8. Interpretation. Having established that the transmitted data set is consistent, the next step is to examine how the individual processors interpret the data. This is accomplished by asking a series of questions:

a. Is the data required for a decision or to populate a data base? If the answer is "no," then the message can be discarded. If the answer is yes, then we proceed to the next question.

b. Is the message accepted correctly by the system? If the answer is "no," then the cause must be determined and rectified. If the answer is "yes," we proceed.

c. Does the system respond correctly to the message? This typically involves populating a track file, initiating a process or providing a status.

9. Information Utilization. Having passed the data and correctly interpreted it, the next step is to verify that the proper action was taken. Errors can take many forms; they include track steals, dropped tracks, misclassifications, fratricide and duplicate engagements. Verification of the action taken involves a review of the logic and code associated with every option that is possible in response to a message or operator action.

V ASSESSMENT PROCESS

Having looked at the parts of the interoperability puzzle, it is possible to develop an assessment process which permits an objective assessment of system interoperability. Several of the steps lead to a "yes/no" or "go/no go" answer. If the answer is negative, there is no interoperability. For those elements in which a calculation is made, interoperability is possible with less than optimum values; however, the interoperability is degraded. Degraded interoperability is most easily considered as operating with an incomplete data set. It is most commonly the result of reduced connectivity or system overload.

Perfect interoperability is possible only in an artificial environment. For operational systems and their models, the measures of interoperability characteristics permit the operational commander and his Joint Interface Control Officer (JICO) to assess, on a continuous basis, the health or interoperability of their systems.

Figure 1 below depicts the process in a single flow chart.

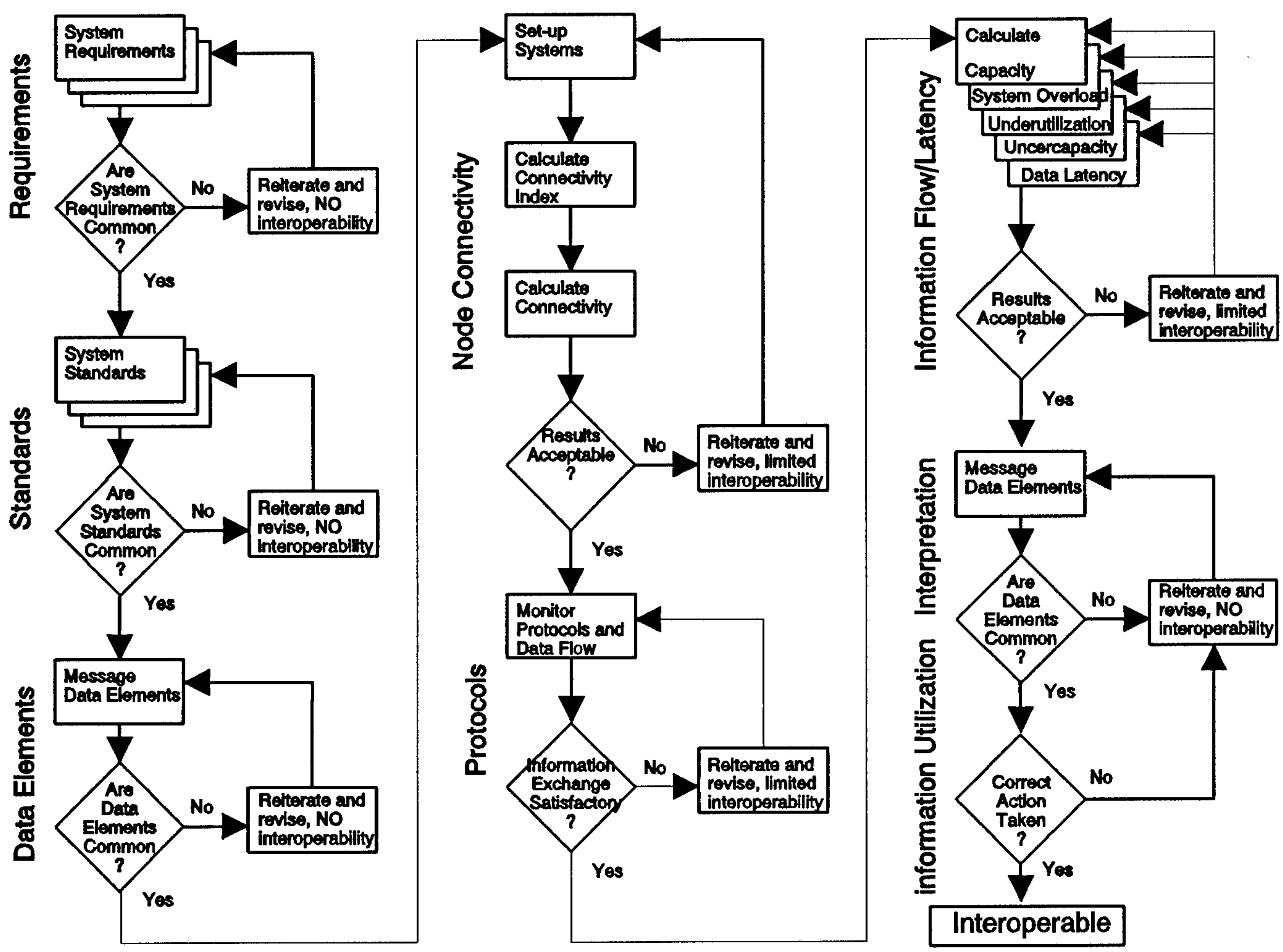

Figure 1. Interoperability Assessment Process

Litton PRC

VI SUMMARY

This paper has shown that system interoperability must be incorporated at the start of the design process, specifically during the generation of system requirements. It is possible to establish a set of characteristics or components which, when taken together, provide an objective assessment of interoperability. The analysis of those characteristics can be adapted to a process or flow chart which may be used by an analyst to determine system interoperability.

REFERENCES

1. CINCLANTFLT message 061415Z FEB 98

2. VCNO letter of 4 Dec 85

3. *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02, Joint Chiefs of Staff, ISBN 0-16-043183-2

4. *SpecWriter*(TM) is a trademark of PRC, Inc, McLean Virginia. DOORS(TM) is a trademark of Quality Systems & Software Ltd, Oxford, UK.

5. *A Fourteen Step Process for Independent Verification and Validation of Models and Simulations*; D. Mensh, M. Leite; PRC, Inc.; Oct 97

6. *Interoperability Methodology*, D. Mensh, 20 Dec 89, (briefing to Space and Naval Warfare Systems Command)

BIBLIOGRAPHY

1. *The Quantification of Interoperability*; D. Mensh, R. Kite, P. Darby; *Naval Engineers Journal*; May 89

2. *Department of Defense Joint Technical Architecture*; Defense Information Systems Agency

3. *C^4ISR Architecture Framework*, Version 2.0; C^4I Integration Support Activity (CISA), Office of the Assistant Secretary of Defense for Command Control, Communication, and Intelligence (OASD[C^3I])